EXHIBIT B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	LEON E. HAUCK, ET AL.	Art Unit 2136
SERIAL NO.:	10/139,924	Confirmation No. 4950
FILED:	May 6, 2002	Examiner: Yalew, Fikremariam A.
FOR:	"METHOD FOR RESTRICTING ACCESS TO A WEB SITE BY REMOTE USERS"	Attny. Dkt. No. 6339-A-1

Certificate of Transmission Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited on February 2, 2006, by first class mail, in the United States Postal Service addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Marvin A. Glazer
By: Marvin A. Glazer, Reg. No. 28,801

Feb. 2, 2006
Date

AMENDMENT

Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action mailed September 2, 2005, please amend the above-identified patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 6 of this paper.

Listing of Claims:

1. (Currently amended) A method of restricting access to data maintained on a server computer by an authorized client machine, said method comprising the steps of:

a. installing a client-side software program on the client machine for generating a client machine-specific identifier, the client machine-specific identifier being unique to the particular machine upon which such client-side software program is initially installed;

b. operating the client-side software program on the client machine to generate the client machine-specific identifier;

c. generating a unique password remote from the client machine, and providing the unique password to a user of the client machine, the unique password being derived from the client machine-specific identifier generated in step b., and uniquely corresponding thereto;

d. issuing a request by the client machine to the server computer for access to data maintained on the server computer;

e. responding to the request for access of step d. by having the client machine re-generate its machine-specific identifier;

f. verifying on the client machine whether the client machine-specific identifier re-generated in step e. uniquely corresponds with the unique password generated in step c.; and

g. recognizing the client machine as being authorized to access data maintained on the server computer if the verification performed by step f. is true, and refusing to recognize the client machine as being authorized to access data maintained on the server computer if the verification performed by step f. is false.

2. Canceled.

3. Canceled.

4. Canceled.

BEST AVAILABLE COPY

5. (Original) The method recited by claim 1 including the step of installing a server-side software program on a server computer, remote from the client machine, for generating the unique password generated in step c. of claim 1.

6. (Original) The method recited by claim 5 wherein the server-side software program is installed on the server computer that maintains the data which the client machine is trying to access.

7. (Currently amended) The method recited by claim 1 wherein the step of generating a unique password remote from the client machine is performed by a computer other than the ~~client machine~~ server computer that maintains the data which the client machine is trying to access.

8. (Original) The method recited by claim 1 wherein the step of installing the client-side software program on the client machine includes the step of downloading the client-side software program from the server computer.

9. (Original) The method recited by claim 1 wherein the step of generating a unique password remote from the client machine includes the step of transmitting the client machine-specific identifier generated in step b. to a password-generating computer other than the client machine, and generating the unique password at the password-generating computer.

10. (Original) The method recited by claim 9 wherein the password-generating computer is the server computer that maintains the data which the client machine is trying to access.

11. (Original) The method recited by claim 9 wherein the password-generating computer operates a software program to perform an algorithm for generating the unique

password based upon the client machine-specific identifier generated in step a.

12. (Original) The method recited by claim 1 further including the steps of:

h. obtaining a session identifier and a site identifier from the client machine each time the client machine requests access to restricted data area of the server computer, the session identifier indicating a particular working session by the client machine, and the site identifier indicating a particular data area of the server computer which the client machine is authorized to access;

i. storing the session identifier and site identifier in a temporary storage table remote from the client machine upon a first request by the client machine for access to a restricted data area of the server computer;

j. comparing the session identifier obtained from the client machine upon subsequent requests for access to the restricted data area of the server following the first request; and

k. allowing the client machine continued access to the restricted data area of the server computer if the session identifier obtained from the client machine upon a subsequent request corresponds to a session identifier already stored in the temporary storage table.

13. (Original) The method recited by claim 1 wherein each client machine is only authorized to access particular data areas of the server computer, and wherein the client-side software program installed on the client machine determines which areas of the server computer can be accessed by a particular client machine.

14. (Currently amended) A method of restricting access to data maintained on a server computer by an authorized client machine, said method comprising the steps of:

a. creating a session identifier in a computer remote from the client machine for a current browsing session of the client machine;

b. transmitting to the client machine the session identifier created in step a);

c. storing the session identifier transmitted in step b) within the client machine;

d. verifying, on the client machine, that the client machine is authorized to access data maintained on the server computer;

e. obtaining the session identifier stored in step c), and storing such session identifier within a storage table remote from the client machine if such client machine was verified in step d);

f. transmitting a request by the client machine for access to data maintained on the server computer, such request including the session identifier stored in step c);

g. comparing the session identifier transmitted in step f) with the session identifier stored in the storage table during step e) to determine whether the request for access transmitted in step f) is authorized; and

h. permitting access by the client machine to the requested data maintained on the server computer if the comparison made in step g) shows that the request for access is authorized, and denying access by the client machine to the requested data maintained on the server computer if the comparison made in step g) shows that the request for access is not authorized.

15. (Original) The method recited by claim 14 wherein the session identifier stored on the client machine in step c) is stored as a temporary file on the client machine.

16. (Original) The method recited by claim 15 wherein the temporary file which stores the session identifier on the client machine is a “cookie”.

REMARKS

This Amendment is responsive to the non-final Office Action mailed September 2, 2005 for the above-identified patent application. The pending claims following amendment are claims 1 and 5-16.

This Amendment is accompanied by a Petition for Two Month Extension of Time, and by payment of the corresponding two-month extension fee for an applicant having small entity status.

Within the Office Action, the Examiner rejected independent claim 1and dependent claims 2-11 and 13, dependent directly or indirectly from claim 1, under 35 U.S.C. §102(e) as claiming subject matter considered by the Examiner to be anticipated by the disclosure within U.S. Patent No. 6,571,339 (Danneels). In view of the amendments made to claim 1 above, such rejection no longer applies, for the reasons explained below.

The cited patent to Danneels (assigned to Intel Corporation) relates to computers using Intel-brand central processors (or "CPUs") that have embedded therein a unique processor identification number. A user computer (402) desiring to access an application or data on a remote server computer (522) first provides its unique processor ID. As shown in Fig. 3 of Danneels, the derivation of this unique processor ID may result from passage of a software module (agent 308/516) from the server to the user's computer; agent 308/516 obtains the unique processor ID and sends it back to a session manager (304/506) in the server computer. As shown in Fig. 5 of Danneels, the server might first send registration pages (510) to the user computer, which the user completes and sends back (512) to the server. Using the registration information (512), the server downloads to the user computer a digital wallet (514); digital wallet 514 may include the aforementioned software module (agent 308/516) that operates on the user's computer to derive the unique processor ID (518). Session manager 506 receives unique processor ID (518) and then downloads a digital membership card (520) to the user computer; digital membership card 520 is based upon the unique processor ID (518) and a unique membership number assigned to such unique processor ID.

Danneels describes the process of validating a request to access a web site at col. 7, line

BEST AVAILABLE COPY

36 to col. 8, line 4. Danneels explains that a user seeking to access a web site provides the user's digital membership card (520). The web site (804), which is maintained on a computer remote from user computer 402, then performs a "validation process" wherein web site 804 retrieves the unique processor ID from the user's computer, and compares it to the unique processor ID contained in the digital membership card (520). In other words, the validation process is performed on the server computer. While Danneels downloads a software module to the user computer 402, the downloaded software module merely serves to detect and transmit the unique processor ID embedded in the CPU of the user's computer.

In contrast, claim 1 as amended recites a method of restricting access to data maintained on a server computer by an authorized client machine wherein the verification step is performed on the client machine, rather than on the server. The method of claim 1 includes the step of installing a client-side software program on the client machine for generating a client machine-specific identifier unique to the particular machine upon which such client-side software program is initially installed; the client-side software program is operated on the client machine to generate such client machine-specific identifier. While such specific identifier could be a unique CPU processor ID, as in Danneels, it need not be so limited. Indeed, basing the client machine-specific identifier upon factors other than just the CPU ID number can safeguard against a scenario wherein a given CPU is shuffled between two or more computer mainboards. The method of claim 1 further includes the step of generating a unique password remote from the client machine, derived from the client machine-specific identifier, and providing the unique password to the client machine.

As further recited in method claim 1, a client machines issues a request to a server computer for access to data maintained on the server computer; such request triggers the client machine to re-generate its machine-specific identifier. A verification step is then performed on the client machine to confirm that the re-generated client machine-specific identifier uniquely corresponds with the unique password previously provided to the user. As explained in Applicants' specification, this verification process is performed, in the preferred embodiment, by a client machine key DLL. If such verification is successful, the client machine is then recognized as being authorized to access data maintained on the server computer.

One might regard Applicants' claimed machine specific identifier as being equivalent to Danneels' unique processor ID number, and one might further regard Applicants' claimed unique password as being akin to Danneels' digital membership card. However, Danneels clearly requires that the verification step be performed on the server computer by the session manager (304/506/606); in contrast, claim 1 requires that such verification step be performed on the user's computer. It is respectfully submitted that it would not have been obvious to those skilled in the art to perform such verification in the generally less-secure environment of the user's computer as compared with the more-secure environment of the server computer.

For the reasons set forth above, claim 1, and claims 5-13 dependent therefrom, as amended, define subject matter that is not anticipated by Danneels, and not obvious in view of the cited art of record. Applicants further note that dependent claim 13 adds the limitation that the client-side software program installed on the client machine determines which areas of the server computer can be accessed by a particular client machine. Applicants' specification, at page 14, lines 6-18, explains that a Java applet installed on the client machine can derive, from the password information, the level of access to which a particular client machine is entitled, and that such authorized access level information is transmitted to the remote server. This feature recited by claim 13 is neither disclosed nor suggested by the cited art.

Within the Office Action, the Examiner rejected independent method claim 14, and claims 15 and 16 dependent therefrom, under 35 U.S.C. §102(b) as describing subject matter considered by the Examiner to be anticipated by U.S. Patent No. 6.092,196 to Reiche. Claim 14 recites a method of restricting access to data maintained on a server computer by an authorized client machine. In practicing such method, a session identifier is created in a computer remote from the client machine for a current browsing session of the client machine. This session identifier is transmitted to the client machine and stored therein. A verification step is performed to determine whether a client machine is authorized to access data maintained on the server computer. As amended, claim 14 recites that this verification step is performed on the client machine. As already noted, Applicants' specification explains that, in the preferred

BEST AVAILABLE COPY

embodiment, the client side software on the client machine performs such verification step by re-generating the machine-specific identifier and comparing it to the unique password saved by the user in the client machine. Assuming that such verification is successful, then the client machine sends the aforementioned session identifier to a remote storage table for use in processing subsequent access requests. Subsequent access requests by a client machine include the session identifier, which is then compared to the session identifier stored in the remote storage table.

Applicants agree that the cited patent to Reiche discloses the concept of generating a session identifier in a server computer and transmitting such session identifier to the user computer. However, in Reiche, verification of each user is performed by an "authentication server" having a database holding user IDs and passwords of authorized users; see col. 5, lines 32-42, and col. 9, lines 15-56. This authentication server is remote from the user's machine. There is no teaching in Reiche, or in any of the other cited art, which would suggest that this verification/authentication procedure be performed by the client machine, as now recited by claim 14, as opposed to being performed by a remote server.

For the reasons set forth above, pending claims 1 and 5-16 define subject matter that is neither anticipated by, nor suggested in view of, the cited art of record. Accordingly, Applicants requests that the Examiner issue an early Notice of Allowance.

Respectfully submitted,

CAHILL, VON HELLENS & GLAZER P.L.C.

Marvin A. Glazer
Registration No. 28,801

155 Park One
2141 East Highland Avenue
Phoenix, Arizona 85016
Ph. (602) 956-7000
Fax (602) 495-9475
Docket No. 6339-A-1

BEST AVAILABLE COPY